정보시스템 보안 시행세칙

2016. 2. 1. 제정
2017. 6. 1. 개정
주무부서 : 기획과

제1장 총칙

제1조(목적) 정보시스템 보안 시행세칙(이하 “본 시행세칙”이라 한다)은 대신대학교(이하 “본 대학교”라 한다) 정보통신자원 이용 및 보호 규정 제3조(정보통신자원 이용 및 보호를 위한 시책의 강구)의 의무에 따라 정보통신센터와 교내 전 부서의 정보시설 및 전산장비에 대한 물리적, 관리적 정보보안을 강화하는 것을 그 목적으로 한다.

제2조(적용 범위) 본 시행세칙은 본 대학교와 연관된 전산장비 및 정보서비스의 운영자 및 이용자를 대상으로 한다.

제3조(용어 정의) 본 시행세칙에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “정보시스템”이란 서버, 스토리지, 네트워크, 어플리케이션 서비스, 단말기 등으로 구성된 정보서비스를 제공하고 이용하기 위한 시스템을 말한다.
2. “정보시스템 관리자”란 정보시스템을 설치하고 운영하는 주무부서의 책임자를 말한다.
3. “정보시스템 담당자”란 정보시스템 관리자가 정보시스템 운영을 위해 지정한 담당자를 말한다.
4. “보안사고”란 보안정책에 위배되는 모든 사고를 말하며 보안 침해사고, 악성코드, 바이러스, 재해 등으로 인한 정보자산의 손상 등을 포함한다.
5. “침해사고”란 권한이 없는 사용자가 비합법적인 방법으로 시스템에 접근하여 시스템의 서비스를 지연시키거나 시스템을 파괴, 데이터를 변조, 삭제하는 등의 행위로 발생한 사고를 말한다.
6. “정보보호시설”이란 전산실, 자료보관실 등 정보시스템 및 개인정보를 보관하는 별도의 물리적 보관 장소를 말한다.
7. “취약성”이란 조직 내부 혹은 정보시스템을 사용하는 환경 등에 내재된 약점으로 위협에 의해서 자산이나 조직의 업무환경에 피해를 가할 수 있는 가능성을 제공하는 요소를 말한다.
8. “단말기”란 정보시스템 및 전산망으로 연결하여 정보시스템을 이용할 수 있도록 한 PC를 말하며, 대부분의 PC가 이에 해당된다.
9. “콘솔”이란 서버 및 네트워크 장비 등의 장애, 로그 등을 직접 표시하고 처리하는 PC를 말한다.
10. “바이러스”란 컴퓨터의 정상적인 동작에 영향을 미치거나 저장된 데이터를 파괴하는 행동을 하는 악성 소프트웨어를 말한다.
11. “백신 프로그램”이란 바이러스 프로그램을 탐지 및 제거하고, 감염된 데이터를 치료하는 프로그램을 말한다.

12. “무결성”이란 정보처리 과정 및 전송 도중에 정보가 불법적으로 변경되지 않고 일관성을 유지하는 것을 말한다.
13. “정보시스템 보안 감사”란(이하 “감사”라 한다.) 정보시스템이 규정 및 보안정책에 준하여 안전하게 운용되고 있는지를 확인하기 위하여 전산시스템 내에 기록·저장되어 있는 각종 사용자 행위에 대한 상세 내용을 조사·분석하는 것을 말한다.
14. “접근통제”란 인가된 사용자, 프로그램, 프로세스, 시스템 등의 주체만이 전산시스템의 자원에 접근할 수 있도록 제한하는 것을 말한다.
15. “전자우편(E-mail)”이란 컴퓨터 통신망을 이용하여 다른 한 사람 또는 여러 사람에게 동시에 정보를 전달하거나 받는 시스템을 말한다.
16. “데이터베이스(DB)”란 여러 개의 파일이나 응용 프로그램에 의해 저장되고 처리되던 자료를 체계적으로 통합하여 모여 있는 형태를 말한다.
17. “DBMS”란 데이터베이스를 구성하고 이를 응용하기 위하여 구성된 관리 시스템을 말한다.
18. “암호화(Encryption)”란 정보의 보안을 유지하기 위해 그 정보를 특정한 규칙에 따라 변형하는 것을 말한다. 이와 반대로 암호화된 문장으로부터 원래의 정보를 복구하는 것을 복호화(decryption)라 한다.
19. “소셜네트워크서비스(SNS)”란 사용자 간 자유로운 의사소통 및 정보공유를 통해 사회적 관계를 생성하고 강화시켜주는 온라인 서비스를 말한다.
20. “클라우드”란 입·출력 작업은 개인이 사용하는 단말기에서 처리되는 것과 대조적으로, 정보분석 및 처리, 저장, 관리, 유통 등의 작업이 이루어지는 원격지의 제3의 공간을 말한다.

제2장 정보보안 조직 및 활동

제4조(정보시스템보안담당관) ① 정보시스템보안담당관은 본 대학교의 보유정보 및 정보통신망을 보호하기 위하여 정보보안 업무를 총괄한다.

② 정보시스템보안담당관은 정보통신센터장으로 하며, 다음 각 호의 업무를 수행한다.

1. 정보시스템보안 정책 및 기본계획 수립
2. 정보시스템보안 관련 규정·시행세칙 등 제·개정
3. 정보화추진위원회에 정보보안 안건 심의 주관
4. 사이버 침해사고 초동조치 및 대응
5. 정보보호 관리실태 평가 및 수준진단
6. 정보보호 예산 및 전문인력 확보
7. 정보보호 전담조직 구성
8. 정보보호 활동계획 수립 및 분석
9. 정보보안 감사
10. 재난방지 대책 수립
11. 대외 협의기구 정보협력
12. 기타 교내 정보시스템 안을 위하여 필요한 행위

제5조(정보시스템보안관리자) ① 정보시스템보안담당관은 본 대학교의 정보보안 업무추진

을 위하여 정보시스템보안관리자를 둔다. 정보시스템보안관리자는 팀원 중 정보시스템보안 담당자를 지정할 수 있으며, 정보시스템보안담당자는 정보시스템 보안관리자의 업무 수행을 보조한다.

② 정보시스템보안관리자는 인프라팀장으로 하며, 다음 각 호의 업무를 수행한다.

1. 정보시스템보안 정책 및 기본계획 시행
2. 정보시스템보안 관련 업무 지도·감독, 감사·심사(검수)분석
3. 데이터센터, 정보통신망 등 통신기반시설 보호 및 보안관리
4. 교내 정보보호 관리실태 점검
5. 사이버위협정보 수집·분석 및 보안관제
6. 정보보안 사고조사 및 처리
7. 정보보호 교육 및 협력
8. 정보보호 전담조직 운영
9. 정보보호 활동계획 이행
10. 모의훈련 계획 및 시행
11. 현장 지도방문 및 상담
12. 사이버보안진단의 날 이행
13. 재난방지 대책 이행
14. 정보보안 표준 적용
15. 기타 교내 정보시스템보안을 위하여 필요한 행위

제6조(부서별 정보보안) ① 각 부서는 기획과 보안규정에 따라 분임 보안담당관을 두어 부서 내 정보보안에 대한 책임을 진다.

② 분임 보안담당자는 다음 각 호의 업무를 수행한다.

1. 부서 정보보안 정책 및 기본계획 시행
2. 부서 정보보안 관련 업무 지도·감독
3. 부서 정보보호 관리실태 점검
4. 부서 관련 사이버 침해사고 처리 협조
5. 부서 내 사이버보안진단의 날 이행 관리
6. 기타 부서 내 정보보안 관련 업무 수행
7. 부서에서 운용하는 정보시스템의 보안관리

제7조(보안책임) ① 사용자는 사용하는 PC 등 소관 정보시스템의 사용, 본인 계정, 정보통신망 접속, 정보서비스를 이용하는 것과 관련한 보안책임을 가진다.

② 정보시스템관리자는 서버·네트워크 장비 등 부서 공용으로 사용하는 정보시스템의 운용과 관련한 보안책임과 각 부서에서 운영하는 정보시스템에 대한 보안통제를 하여야 한다.

③ 정보시스템을 실제 운영하는 부서의 장과 정보시스템담당자는 해당 정보시스템의 운영과 서비스에 대한 보안책임을 가진다.

④ 정보시스템보안관리자 및 정보시스템보안담당자는 제1항 내지 제3항에 명시된 정보시스템 운용과 관련한 보안대책 강구가 필요하다가 판단할 경우, 정보시스템관리자 및 담당자에게 시정을 요구할 수 있다.

제3장 사이버 침해사고 대응

제8조(사이버 침해사고 및 위기 대응) ① 사이버 침해사고 발생으로 간주할 수 있는 적용 범위는 다음 각 호와 같다.

1. 해킹, 웜바이러스 유포 등 사이버공격으로 인한 학교 및 국가 정보통신망의 마비, 기밀·개인정보 등 중요자료 유출 등 사이버 위기상황 발생 시
2. 교육부의 사이버 위기 대응 활동에 부합하는 경우
3. 사이버 공격이 광범위하게 발생하여 총괄·종합적인 대응이 필요한 경우

② 사이버 침해사고는 그 위기형태에 따라 다음 각 호와 같이 분류할 수 있다.

1. 인터넷을 통해 교내 전산망에 직접 침투하여 전산망 교란 및 재침투를 위한 백도어를 설치
2. 홈페이지, 메신저, 전자우편 등을 활용하여 악성코드를 유포하고 교내 정보시스템 및 PC에 저장된 데이터 및 개인정보를 조작·파괴·은닉·절취 및 탈취
3. 봇넷(Botnet) 구축 등 서비스거부공격을 통해 대량 데이터전송·부정명령 등으로 시스템 및 전산망의 정상동작을 방해
4. 국가 사이버 위기 경보 발령

구분	판단기준	비고
정상 (Green)	○ 위험이 없는 평상시 ○ 위험 정도가 낮은 웜·바이러스, 해킹기법, 보안취약점이 발견	-
관심 (Blue)	○ 위험도가 높은 웜·바이러스, 취약점 및 해킹 기법 출현으로 피해 발생 가능성 증가 ○ 해외 사이버 피해가 확산되어 국내 유입 우려	활동 감시
주의 (Yellow)	○ 일부 정보통신망 및 정보시스템 장애 ○ 침해사고가 일부기관에서 발생했거나 다수기관으로 확산될 가능성 증가 ○ 국가 정보통신기반시설 전반에 보안태세 강화 필요 ○ 국내·외 정치/군사적 위기상황 조성 등 사이버안보 위해 가능성 고조	협조 체제 가동
경계 (Orange)	○ 복수 정보통신서비스제공자(ISP)망/주요 통신망 장애 발생 또는 마비 ○ 침해사고가 다수기관에서 발생했거나 대규모 피해로 발전될 가능성 증가	대비 계획 점검

	○ 다수 기관의 공조 대응 필요	
심각 (Red)	○ 국가 차원의 주요 정보통신망 및 정보통신 기반 시설 운영 마비 ○ 침해사고가 전국적으로 발생했거나 피해범위가 대규모인 사고 발생 ○ 국가적 차원에서 총력 대처 필요	즉각 대응 태세 돌입

③ 정보시스템보안담당관은 침해사고 발생 시 사이버침해사고대응반을 구성하여 대응한다.

업무	임무	담당
대응반장	○ 사이버침해사고대응반 운영 총괄 ○ 대응계획 수립 및 대응결과 종합 ○ 피해복구계획 수립 및 복구 현황 점검	전산담당부장
보안관제	○ 네트워크 이상 징후 감시 ○ 피해상황 접수 및 초동조치 ○ 국내·외 주요 보안사이트 모니터링 ○ 네트워크 장비 보안강화 ○ 정보보호 시스템 모니터링 및 차단	전산담당부장 정보보호담당자 네트워크담당자
사고대응	○ 사이버침해 피해시스템에 대한 국가정보원 또는 ECSC 악성코드 샘플채취 지원 ○ 사이버 피해분석을 위한 시스템 로그 보존 및 분석 ○ 각 시스템 보안패치 및 컴퓨터 백신 업데이트	전산담당부장 정보보호담당자 네트워크담당자 서버담당자
대외협력	○ 사이버위기 경보 수신시 기관 내 전파 ○ 교육사이버안전센터에 상황 통보 ○ 교육부 긴급대응반 또는 사고대책본부와 유기적 협조	전산담당부장 정보보호담당자

④ 사이버 침해 및 보안사고 발생 시 정보시스템보안관리자는 다음 위기대응 절차에 따라 대응한다.

상황	내용	처리절차	비고
접수	사고인지 및 접수	신고접수(ECSC, 피해자신고 등) 및	중요 사안은

			자체점검	상급자 보고 신고양식:붙임 #1
조사	사고조사 및 분석 담당자 배정		일시, 장소/사고원인, 피해현황/ 사고자 및 관계자 인적사항, 운영환경 등 조사	중요 사안은 상급자 보고, 외부공격은 ECSC 신고
조치	대상별 전파/조치 (유선/매일/공문)	서버/ 웹서비스	각 정보시스템담당자에 대한 사고사항 전파 및 조치 가이드	
		네트워크/ 보안	네트워크/보안시스템 확인	
		PC	PC클리닉 접수/조치	
점검	대상별 결과점검	서버 웹서비스	정보시스템담당자 사고 시스템점검 및 조치사항 회신 통보	필요 시 IP/계정/도메인 차단
		네트워크	네트워크/보안시스템 점검	
		PC	사고 PC점검/온료 (경과별 운영일지 기록)	
종결	종결처리 및 피드백		종결처리(ECSC, 자체) 후속 조치 담당자별 피드백	중요 사안은 상급자 보고

⑤ 기타 사이버 침해사고 대응은 교육부 사이버분야 위기대응 실무 매뉴얼을 준용한다.

제9조(정보시스템 침해 대응 절차) ① 정보시스템관리자 및 담당자는 로그 점검 혹은 실시간 모니터링을 수행할 때 다음 각 호에 유의하여 침입자의 침입흔적을 확인한다.

1. 같은 사용자 이름으로 두 명 이상의 동시 로그인이 되고 있는지 확인한다.
2. 예측 가능한 정규 시간외의 시스템 사용자를 확인한다.
3. 관리자 권한 외의 작업수행 시도가 있었는지 점검한다.
4. 보안 관련 파일의 수정 및 수정 시도가 불법적으로 이루어졌는지 점검한다.
5. 허가가 안된 파일, 서비스 및 기타 자원의 접근 시도를 확인한다.
6. 일반 사용자의 홈 디렉토리, 임시 디렉토리에 시스템 또는 숨김 파일이 존재하는지 확인한다.
7. 계정 관련 시스템 파일에 관리자 이외의 접근 시도가 있었는지 점검한다.
8. 네트워크 전송량을 증가시키는 비정상적인 프로그램 실행 작업이 있는지 점검한다.
9. 한 사용자가 많은 외부 접속을 시도하고 있는지 점검한다.
10. 허가된 IP 사용자가 아닌데 로그인을 하려는 시도 및 접속을 점검한다.
11. 시스템의 비정상적인 동작이 있다면 외부의 불법적인 침입이 있는지의 여부를 점검

한다.

12. 침입의 흔적을 발견 시 그 원인이 운영 및 개발부서의 담당자나 개발자의 실수 때문인지 확인한다.

② 정보시스템담당자는 침입자가 시스템 내에서 활동하고 있는 것으로 판단될 경우 다음 각 호에 따라 조치한다.

1. 정보시스템담당자는 즉시 정보시스템보안담당자 및 소속부서 팀장에게 보고하고, 정보시스템보안담당자는 사안의 중요도에 따라 정보시스템보안담당관에게 보고한다.
2. 정보시스템보안담당관은 필요 시 관련 외부 공공기관 및 상급기관의 협조를 받기 위한 절차를 준비한다. 이때, 협조 의뢰의 최종 결정은 정보시스템보안담당관이 한다.
3. 침입자의 시스템 내 활동을 발견 시 정보시스템담당자의 세부 처리절차는 다음 각목과 같다.

가. 내부 단말기에서 침투한 경우 현재의 단말 위치를 확인한다.

나. 현재 침입자가 시스템 내에 있다면, 가능한 도구나 명령어를 이용하여 침입자에 관련된 정보를 수집한다.

다. 침입자가 수행하고 있는 명령어를 파일로 저장하거나 기록한다.

라. 침입자가 중요한 데이터에 접근을 할 경우 또는 침입자에 대한 추적이 용이하지 않을 경우 침입자의 연결을 끊는다.

4. 정보시스템담당자는 침입자의 시스템 내 활동에 대한 절차 적용 후 보안사고 및 대응결과를 문서로 작성하여 정보시스템보안담당자에게 제출하고, 정보시스템보안담당자는 이를 정보시스템보안관리자 혹은 담당관에게 보고한다.

③ 정보시스템담당자는 시스템 내 침입흔적 발견 시 다음 각 호에 따라 조치한다.

1. 로그 파일의 분석 등을 통해 침입한 흔적이 발견된 경우 보안진단 도구나 체크리스트를 이용하여 다음 각 목과 같은 사항을 점검한다.

가. 새로운 계정이 생성되어 있는지 확인한다.

나. 패스워드 파일이 변경되었는지 확인한다.

다. 주요 설정 및 실행 파일 등이 변경되었는지 확인한다.

라. 특정 파일의 접근 모드가 변경되었는지 확인한다.

마. 시스템 유틸리티가 변경 및 수정되었는지 확인한다.

2. 데이터의 변조나 불법 접근의 흔적이 있을 경우 해당 서비스를 중지시킨다.
3. 침입자를 식별하기 위한 증거 수집을 한다.
4. 백업 등을 이용하여 복구한다.
5. 정보시스템담당자는 침입흔적 발견 후 피해상황을 파악하여 보안사고 및 대응결과서를 작성한 뒤 정보시스템보안담당자에게 통보한다.

④ 정보시스템보안담당자는 정보시스템담당자의 협조를 받아 다음 각 호에 따라 조치한다.

1. 침해사고 발생시 정보시스템보안담당자의 세부 업무 처리 절차는 다음 각 목과 같다.

가. 침해사고의 피해 상황을 파악한다.

나. 침입자를 식별하기 위한 증거를 수집한다.

다. 시스템의 복구여부를 확인한다.

라. 문제점을 파악하여 대책을 제시한다.

마. 필요 시 교육사이버안전센터 및 사이버 보안관련 주무 정부기관에 침해사고를 접수한다.

2. 보안사고 및 대응결과와 보안사고 발견 및 조치를 문서로 작성한다.
3. 보안사고 기록은 대외비로 분류하고 1년 이상 보관한다.
4. 교육 및 홍보를 강화하고 동일 문제가 재발하지 않도록 권고한다.

제10조(보안취약성 대응 절차) ① 정보시스템담당자는 주기적으로 시스템을 모니터링하여 시스템이나 소프트웨어의 보안취약성을 파악하고, 필요 시 정보시스템보안담당자에게 그 결과를 통보한다.

② 정보시스템담당자의 보안취약성 발견에 따른 대응절차는 다음 각 호와 같다.

1. 정보시스템담당자는 보안취약성 발견 시 다음 각 목과 같이 대응한다.

가. 화면상의 메시지들 또는 로그 결과들에 대하여 기록 또는 별도 저장한다.

나. 컴퓨터를 네트워크와 분리시키고 작업을 중지한다.

다. 정보시스템 취약성에 대해 점검한다.

라. 필요 시 취약성 검사도구, 백신 소프트웨어를 이용하여 점검하며, 시스템 패치가 있는 경우 이를 적용한다.

마. 용도가 분명하게 파악되기 전까지 설치된 소프트웨어를 임의로 제거하지 않는다.

2. 정보시스템보안담당자는 필요 시 보안취약성에 대한 조치결과를 별도로 문서화하여 보관한다.

제4장 정보보호시설 보안

제11조(데이터센터 보안) ① 정보통신센터장은 교내 중요 정보자원을 보호하기 위하여 데이터센터를 출입통제구역으로 정하고 다음 각 호에 따라 관리하여야 한다.

1. 데이터센터는 방수, 방화, 방진, 초음파 도청 및 외부 침입 방지 등 전산실 요건에 가장 부합하는 건물 또는 사무실에 위치해야 한다.
2. 데이터센터는 지진지대, 침수지대, 위험물(폭발물, 가스, 유류 등) 보관 장소 등 재난 발생우려 지역이 아닌 곳에 위치해야 한다.
3. 데이터센터의 출입사항은 무인 감시카메라 또는 출입 자동기록 시스템에 의해 사후 확인이 가능하도록 하여야 한다.
4. 데이터센터 재난에 대비하여 열 감지기, 연기감지기, 누수감지기 등의 방화시설, 하론가스 등 소화설비, 기타 방재설비를 적절히 보유하고 있으며, 작동 가능한 상태로 유지해야 한다.
5. 데이터센터에는 항온·항습을 유지할 수 있는 설비를 설치하며, 적절히 운영하여야 한다.

② 데이터센터는 비상 시 인명 및 시설물 안전에 대비하기 위하여 다음 각 호의 조건이 충족되어야 한다.

1. 화재 시 사람이 대피할 수 있도록 경고, 비상벨 등이 먼저 울리고 일정시간 이후에 자동 소화 설비가 작동되도록 해야 한다.
2. 비상 시 작업인원이 대피할 출입구가 존재해야 한다.
3. 데이터센터 천장 및 바닥에 대형 수도관 등이 통과하지 않도록 한다.
4. 데이터센터 화재 시 자동 작동되는 소화설비에 전산장비에 치명적인 물을 분출하는 스프링쿨러가 포함되어서는 안된다.

5. 비상사태 발생 시 빠른 복구를 위해 데이터센터 내에 비상연락망을 항시 비치하여야 한다.

③ 데이터센터 내 안정적인 전원공급을 위하여 다음 각 호에 따라 무정전시설(UPS)이 관리되어야 한다.

1. 데이터센터에는 무정전시설을 설치해야 한다.
2. 무정전시설의 용량 및 품격은 시설관리부서의 공인을 받아야 한다.
3. 정전 등 비상시에도 데이터센터를 안정적으로 운영할 수 있도록 전원배선은 타 사무실용과 분리하여 운영하여야 한다.
4. 시설관리부서의 담당자는 발전기를 유지관리하며, 주기적으로 시험 가동해야 한다.

④ 데이터센터 내의 정보시스템 자산은 다음 각 호에 따라 관리되어야 한다.

1. 인프라팀장은 정보통신센터 내의 전산장비, 통신장비, 부대설비에 대한 목록을 관리하여야 하며, 항상 최신의 자료를 유지하여야 한다.
2. 정보통신센터 내의 전산장비(PC, 서버, 스위치, 허브, 무정전시설 등) 및 부품의 교체나 철수 시는 반드시 그 품목과 내용을 확인하고, 장비 반·출입 관리대장에 기록한다.
3. 데이터센터 내 중요 전산장비는 전원 스위치를 덮개 등으로 보호하여 사람들의 이동시 등 예기치 않은 문제로 전원이 꺼지는 경우를 방지한다.

⑤ 데이터센터 내 콘솔실은 다음 각 호에 따라 관리되어야 한다.

1. 콘솔실 내 모든 저장매체는 통제되어야 하며, 외부 반출시 사전에 담당자의 허가를 득하여야 한다.
2. 시스템 및 업무담당자 외에는 콘솔 및 단말기를 사용할 수 없으며, 부득이 사용할 경우 담당자의 승인을 받은 후 사용할 수 있다.
3. 콘솔실 내 콘솔 및 단말 PC를 조작해서 일어나는 모든 사항에 대한 보안책임은 담당자와 조작한 자가 책임을 진다.
4. 콘솔 조작 중 화면상 식별 가능한 명령 외에는 입력해서는 아니 되며 실행을 위한 엔터키를 입력 전에는 명령 재확인과정을 거쳐야 한다.
5. 콘솔실에는 음료 등을 반입할 수 없으며 외부에서 사용하는 신발 등을 착용할 수 없고, 항시 청결하게 유지하고 정숙하여야 한다.
6. 콘솔에 대해 물리적 접근통제(잠금장치 설치, 접근통제가 되는 장소에 설치 등)를 실시하여야 한다.
7. 시스템 단말기에 대하여 다음 각 목의 사항을 반영한 논리적 접근통제를 실시한다.

가. 사용자 인증
나. 자동 타임아웃(time-out) 또는 로그오프
다. 이용 시간대 통제
라. 단말기 확인 및 인증
마. 작업 로그
바. 비밀번호 및 중요 데이터 전송 시 암호화
사. 시스템의 접근시도 제한횟수 초과 시 사용 중지
아. 기타 특이사항 출력

⑥ 데이터 백업시스템 운용을 위한 데이터 백업실은 다음 각 호에 따라 관리되어야 한다.

1. 데이터 백업실은 잠금 장치를 설치하며 담당자와 담당자의 승인을 받은 자만 출입을 허가한다.

2. 작업 계획에 의한 소산 소요분만 반출하고 소산된 테이프의 수량과 반출된 수량이 동일한지 확인한다.
3. 소산 및 반출용 테이프는 백업매체 관리대장에 백업담당자가 상세히 기록하고 직접 반·출입한다..
4. 데이터의 파괴, 유출, 변조 등을 방지하기 위하여 필요 시 중요 데이터는 2개의 복사본을 추가로 만들어 보관한다.
5. 데이터 백업실 운영자는 각 테이프별로 데이터 내용을 정리하여 보관하여 한다.
6. 재해 대비용 테이프는 소산장소의 자체 보관함에 따로 보관한다.

⑦ 정보통신센터장은 프린터실(고속프린터)을 출입제한구역으로 지정하고 다음 각 호에 따라 관리하여야 한다.
1. 중요자료 파기 시에는 담당자 입회하에 분쇄기에 파기하여야 한다.
2. 비인가된 외부인의 프린터실 출입을 통제하여야 한다.
3. 반출되는 모든 출력물은 출력물 배포 대장에 기록하며 외부 및 현업 부서 발송용 출력물은 담당자가 별도의 양식에 서명 후 배포한다.

⑧ 데이터센터 내 네트워크 장비실은 다음 각 호에 따라 관리되어야 한다.
1. 네트워크 장비실의 시건장치를 항상 확인한다.
2. 전산망에 접속하는 단말기 취급자를 구별하여 인가된 직원에 한하여 접속을 허가한다.
3. 네트워크 장비 반·출입시 운영자의 허가를 취득한 후 반·출입하며 정보통신센터 직원 외 담당자의 허가를 득하지 않은 인원은 네트워크 장비를 사용할 수 없다.

제12조(출입통제 및 제한) ① 정보보호시설에는 다음 각 호를 적용하며, 책임자를 지정하여야 한다.
1. 출입통제구역은 데이터센터 및 데이터 백업실로 한다.
2. 출입제한구역은 출입통제구역 외 정보통신센터에서 관리하는 모든 호실로 한다.
3. 출입자는 보안구역에 따라 출입인가 등록을 받은 자에 한한다.
4. 정보통신센터의 모든 호실에는 출입을 통제하는 시건장치를 설치한다.
5. 정보통신센터의 모든 호실은 관리책임자를 정한다. (아래는 예시임)

호실번호(호실명)	관리책임자(정)	관리책임자(부)
	정보통신센터장	담당팀장

② 정보보호시설에 대한 출입자격은 다음 각 호를 따른다.
1. 정보시스템 운영의 사고예방을 위하여 외부인의 정보통신센터(데이터센터 내 정보시스템실, 네트워크 장비실, 데이터 백업실 등이 포함된다.)의 출입은 제한된다. 예외적으로, 정보통신센터 근무자 및 상급관리자는 출입이 허용된다.
2. 정보통신센터 담당자의 사전승인을 받은 자로서 다음 각 목의 해당자는 출입이 허용된다.

가. 관련 시스템의 테스트가 필요한 경우
나. 장애발생시 시스템 유지보수 및 개발 담당자에 의한 복구가 필요한 경우
다. 전산설비 설치 및 관리 상 출입이 필요한 경우

라. 책임자의 사전승인을 득한 시설(설비) 보수, 개수 작업자 작업 시

③ 정보보호시설에 대한 출입절차 및 출입자 관리는 다음 각 호를 따른다.

1. 출입통제구역에 대한 출입이 필요한 경우 출입희망자는 정보통신센터 담당자의 사전 허가를 받아야 한다.
2. 정보통신센터 직원은 별도의 출입요청서 없이 수시 출입이 가능하나 협력사 관계자의 출입이 필요한 경우 출입요청서를 작성한 후 출입하여야 한다.
3. 데이터센터 관리 담당자는 정보통신센터 출입승인을 득한 자에게만 출입을 허용하여야 하며, 업무 담당자는 출입에 동행하여야 한다.
4. 데이터센터 관리 담당자는 출입자에 대하여 출입사항을 출입대장에 기록하도록 한다.
5. 출입자 관리기록부는 주 단위 또는 월 단위로 인프라팀장에게 결재를 득하며 보관기간은 1년으로 한다.
6. 데이터센터의 출입사항은 무인 감시카메라 또는 출입통제시스템에 의해 사후 확인이 가능하도록 하여야 한다.
7. 정보보호시설 출입자는 시설 내에서 사진 및 동영상 촬영을 금지하며, 촬영이 필요한 경우 정보시스템보안관리자의 허가를 득하여야 한다.

제13조(데이터센터 보안점검) 데이터센터 관리자는 정기적인 보안점검을 실시하고, 그 결과를 인프라팀장에게 보고하며 인프라팀장은 보안점검의 적정성을 확인한다.

제5장 네트워크 보안

제14조(네트워크 보안) ① 본 대학교 내 네트워크는 다음 각 호를 따라 구성되어야 한다.

1. 네트워크 구성 및 보안시스템과 관련된 정보(노드, IP주소, 관리자 암호 등)에 관한 접근을 통제한다.
2. 네트워크 관리를 위한 데이터 덤프, 추적 및 진단 데이터 파일은 허가되지 않은 접근으로부터 보호되어야 한다.

② 교내 IP 할당 체계는 다음 각 호를 충족하여야 한다.

1. IP 주소를 데이터베이스화 하여 일원적으로 관리한다.
2. IP 주소의 변경은 관련 담당자들에게 통보한 후 실시한다.
3. 일반 사용자들은 PC의 IP 주소를 임의로 변경할 수 없다.
4. 내부망에는 공인 및 사설 IP를 사용하나, 보안정책에 따라 구분하여 적용할 수 있다.

③ 네트워크 담당자는 네트워크 진단/관리 도구를 이용하여 보안상태를 진단하여야 한다.

1. 네트워크 부하를 모니터링하고 분석하여 최적의 상태를 유지하기 위해 네트워크 진단/관리 도구를 사용한다.
2. 네트워크 진단/관리 도구의 사용 시 진단 포트가 열려 보안에 취약성이 발생할 수 있으므로 진단 포트에 대한 불법적인 접속 여부에 대해 점검을 실시할 수 있다.
3. 네트워크 진단/관리 도구들은 네트워크 관리 담당자에 의해서만 사용될 수 있으며 일반 사용자들에게는 사용이 허가되지 않는다.

④ 네트워크담당자는 정보보호가 필요한 노드에 대해 적절한 네트워크 접근 경로를 정의한다.

1. 정보시스템의 중요정보에 접근이 필요한 단말기는 접근통제가 되거나 사전 등록된 IP

를 사용한다.

2. 내부 사용자는 침입차단시스템 등 보안시스템의 경로를 우회하는 경로를 설정해서는 아니되며, 부득이 한 경우 인프라팀장과 정보시스템보안담당자의 승인을 득한 후 사용한다.

3. 네트워크 사용자는 승인없이 개인 소유의 컴퓨터, 주변 장치 또는 소프트웨어를 교내로 가져와서 네트워크에 연결해서는 아니 되며, 개인 PC 등록절차는 “전산기자재 관리 시행세칙”을 따른다.

⑤ 네트워크를 통한 보안사고 예방, 수사, 감사 등의 목적으로 네트워크 연결 시 사용자 인증을 사용하도록 하며, 필요 시 다음 각 호의 정책을 적용할 수 있다.

1. 인터넷을 통한 모든 접속을 로깅한다.
2. 원격 사용자의 정보시스템 접속을 위한 인증은 암호화되어야 한다.
3. 원격 사용자에 의한 접속은 인증되어야 한다.
4. 내·외부 네트워크간의 접속은 보안 기능에 의하여 통제할 수 있다.
5. 인터넷과의 연결지점에 침입차단의 목적으로 방화벽, 침입차단시스템 등 별도의 보안장비를 설치할 수 있다.

⑥ 네트워크에 연결된 네트워크 및 보안장비의 물리적 보안을 위해 다음 각 호의 사항을 이행하여야 한다.

1. 네트워크 설비 또는 장비는 허가되지 않은 물리적 접근으로부터 보호하기 위하여 잠금장치가 되어 있는 장소에 설치를 한다.
2. 통신망 및 관련 주요 장비는 무정전 시설 확보, 비상전원 확보, 공조장치, 환풍장치, 냉난방장치, 정전기 방지장치, 소화장비 등의 부대설비를 갖춘 곳에 설치한다.
3. 외부 사람이 출입통제구역 내 네트워크 설비가 설치되어 있는 장소에서 작업을 할 경우 담당자가 동행을 수행하며 출입 일지에 기록한다.
4. 통신회선의 설치를 위한 작업은 인프라팀장의 승인 후에 수행되어야 한다.
5. 허가되지 않은 장비의 네트워크 접속을 탐지하기 위하여 관리시스템을 이용할 수 있다.
6. 사용하지 않거나 불필요한 모든 통신 장비 및 네트워크 세그먼트는 물리적으로 네트워크상에서 접속을 차단한다.

⑦ 네트워크에 연결된 네트워크 및 보안장비에 대하여 다음 각 호를 수행하는 논리적 접근통제가 이루어져야 한다.

1. 허가된 자만이 허가된 네트워크에 접근하여 허가된 작업만 할 수 있도록 네트워크 접근 권한 리스트를 보유한다.
2. 필요시 네트워크에의 접근시간을 제한할 수 있다.
3. 네트워크 장비에 로그인시 반드시 사용자 인증을 수행한다.

⑧ 네트워크 보안사고 발생 시 제3장 침해사고 대응을 적용한다.

⑨ 네트워크담당자는 필요 시 네트워크 보안점검을 수행한다.

제15조(외부 접속) ① 네트워크를 통한 교내외 간 접속이 있을 경우, 해당 정보시스템 업무담당자는 다음 각 호를 고려하여야 하며, 정보시스템보안담당자와 네트워크담당자의 의견을 수렴하여야 한다.

1. 외부로부터의 내부 네트워크 접속 요청 시 보안 사항을 먼저 검토한다.
2. 외부와의 연결은 신뢰할 수 있는 대상으로 한정한다.

3. TCP/IP를 통한 외부와의 연결은 반드시 침입차단시스템을 통하여 연결되어야 한다.
4. 기타 공용망과의 연결은 보안에 최대한 중점을 두어 설계하도록 한다.

② 네트워크를 통하여 민감한 중요 정보의 전송이 필요한 경우 다음 각 호 사항이 준수되어야 한다.

1. 인터넷을 통한 비밀정보 전송 시 암호화한다.
2. 내부망에서도 민감한 정보의 보호가 필요할 경우 적절한 암호화 대책을 수립하여야 한다.
3. 암호화는 네트워크 장비상의 암호화를 구현하거나, 상황에 따라 적절한 프로그램상의 암호화를 고려한다.
4. 암호화 장비 및 도구를 도입할 경우 장비 및 알고리즘은 가능하면 국가나 보안관련 기관의 법적, 규제적 요구를 만족시켜야 한다.
5. 암호화에 사용되는 키 값은 외부에 노출되지 않도록 철저히 관리한다.

제6장 PC 및 단말기 보안

제16조(단말기 보안관리) ① 본 대학교의 모든 단말기 사용자는 PC 등 단말기 사용과 관련된 일체의 보안관리 책임을 가진다.

② 업무 및 연구와 관련된 PC 사용자는 보안성 향상을 위해 비밀번호를 설정하여야 한다.

1. CMOS에서 비밀번호를 설정함으로써 PC 부팅 시 논리적인 접근통제가 이루어지도록 한다.
2. CMOS 비밀번호는 PC 사용자만이 알 수 있도록 설정한다.

③ 모든 PC는 화면보호기를 설정하여 사용자가 잠시 자리를 비운 사이(10분 이상)에 비인가자가 그 PC을 이용하여 작업하는 것을 방지하여야 한다.

1. 화면보호기는 적절한 비밀번호로 보호되어야 하며 화면보호기의 비밀번호는 정보시스템 서비스용 비밀번호와 다른 것을 사용하도록 한다.
2. 화면보호기는 운영체제에서 기본적으로 제공하는 것을 사용하도록 한다.
3. 시스템관리 목적상 제약이 발생되는 조건에서는 예외로 한다

④ 교내 모든 PC는 파일공유를 하지 않는다. 단, 업무상 파일공유가 필요한 경우, 다음 각 호를 준수하여야 한다.

1. CAUDISK를 통한 업무 상 파일공유만 가능하며, 임의로 파일을 공유하지 않는다.
2. 행정부서 임의로 NAS, 파일서버 등의 네트워크 공유시스템을 운영하지 않는다.
3. 업무상 필요한 경우라도 개인 PC에 공유설정을 하지 않는다.

⑤ PC 사용자는 PC 내 데이터 보관 시 다음 각 호에 유의하여야 한다.

1. 일반 사용자의 접근이 가능한 PC는 비밀정보의 노출 위험이 존재하므로 가능한 비밀정보를 파일로 보관하지 않는다.
2. 비밀정보는 접근권한이 설정되어 있는 정보 서버에 저장되는 것을 원칙으로 한다.
3. 업무상 부득이하게 비밀정보를 저장해야 하는 경우 파일에 대한 비밀번호 설정 혹은 암호화 등 보안성을 확보한 후 저장하여 보관한다.
4. P2P 등 파일공유 프로그램을 이용하여 파일을 공유 및 다운로드하지 않으며, PC에 유사 소프트웨어를 설치하지 않는다.

⑥ PC를 통한 인터넷 사용 시 다음 각 호의 사항을 유의하여야 한다.

1. 인터넷을 통한 외부 웹사이트 및 시스템 접속 시 내부에서 사용하는 아이디와 비밀번호를 사용하지 않는다.
2. 운영체제 및 웹 브라우저의 각종 보안 패치 및 서비스 팩을 설치한다.
3. 다음 각목의 사이트는 악성코드 및 바이러스 감염의 소지가 있으므로 접속하여서는 아니 된다.
가. 음란 사이트 : 음란사진, 동영상 등을 제공하는 사이트
나. 무단 복제 사이트 : 무단 복제된 프로그램이나 파일을 제공하는 사이트
다. 해킹 사이트 : 해킹과 관련된 정보를 담고 있는 사이트
라. 도박 등 기타 접속 금지의 필요성이 인정되는 사이트
4. 사용자는 신뢰할 수 있는 웹 사이트를 방문한 경우를 제외하고는 자바와 웹 브라우저의 플러그인 방식의 프로그램 기능 사용에 주의해야 한다.
5. 웹사이트 접속이 팝업되는 창에 '예(Yes)'로 하기 전 그 내용을 상세히 파악함으로써 자바 스크립트, Active-X 공격 등에 노출될 수 있는 가능성을 줄여야 한다.
6. 심각한 악성 자료를 포함하는 사이트를 발견했을 경우, 해당 사이트의 URL을 반드시 회사 웹 보안 담당자에게 통보하여 해당 사이트의 접근을 침입차단시스템에서 제한 하도록 한다.

⑦ PC 사용자는 바이러스 감염방지를 위해 다음 각 호의 사항을 준수하여야 한다.
1. 비 인가된 소프트웨어 및 불법 소프트웨어 사용을 금지하며, 소프트웨어와 관련된 사항은 "소프트웨어 관리 시행세칙"을 따른다.
2. 외부 네트워크나 매체로부터의 파일이나 소프트웨어를 다운로드 받을 경우 바이러스 백신 프로그램을 적용한 후 사용한다.
3. 바이러스 백신 프로그램이 PC 기동 시 자동으로 실행되도록 하고, 바이러스 백신 프로그램은 1일 1회 이상 정기적으로 업데이트를 수행한다.
4. 중요한 업무 프로세스를 지원하는 시스템의 소프트웨어 및 데이터는 주기적으로 점검하여 허가되지 않은 파일이나 수정사항 등이 있는지 조사한다.
5. 전자우편 첨부 파일에 대한 바이러스 감염 여부를 점검한다.
6. 소프트웨어가 바이러스에 감염되는 것을 방지하기 위해 원본 소프트웨어는 쓰기 방지가 되어 있어야 한다.
7. 특별한 이유없이 시스템 혹은 어플리케이션이 동작하지 않을 경우 사용하던 파일을 다른 기계에서 읽거나 실행해서는 안되며 즉각 담당자에게 통지한다.
8. 정보시스템의 바이러스 감염 시 즉각 담당자에게 통지한다.

⑧ PC 사용자는 소프트웨어에 대해 서비스 팩 및 패치 설치를 하여야 하며, 다음 각 호에 유의하여야 한다.
1. 운영체제 및 응용프로그램 제조사가 제공하는 최신 서비스 팩 또는 패치를 설치한다.
2. 서비스 팩이나 패치를 설치할 때는 반드시 제공업체에서 제시하는 주의사항을 명확히 이해한 후 설치한다.
3. 서비스 팩 및 패치 설치 시, 현재 시스템이 운영중일 때에는 가능한 설치하지 않도록 하고 업무가 이루어지지 않는 시간에 실시한다.

⑨ 정보화자산 담당자는 본 대학교 구성원의 PC 사용에 대해 다음 각 호의 사항을 검토하고, 필요시 구성원이 이행하도록 권고하여야 한다.
1. 주기적으로 바이러스 최신정보, 최신 웹 브라우저, 패치 등에 관한 정보를 구성원에게

제공하며, 불법 소프트웨어의 점검을 수행한다.

2. 정보화자산에 대한 자산관리를 수행한다.

3. 인력 퇴직 및 PC 반납 시 반납 PC의 정보는 완전 포맷(Low-level Format) 또는 디스크를 복구 불가능한 형태로 파기한다.

⑩ PC 외 단말기(노트북, PDA, 타블렛, 스마트폰)를 사용하는 경우 PC와 동일한 보안관리 수준을 적용하여야 한다.

제7장 정보시스템 보안

제17조(호스팅 운영) 본 대학교의 웹호스팅, 빌더 및 서버호스팅은 “서버관리 운용 시행세칙”을 따른다.

제18조(계정 운영) ① 본 대학교 내 운영되는 모든 서버 및 정보서비스에 대해 각 정보시스템 담당자는 다음 각 호를 준수하여 계정을 운영하여야 한다.

1. 개별적인 사용자 계정 등록이 필요한 서버는 별도의 사용자 계정 등록(신규, 추가, 삭제) 신청서 제출 등의 계정신청 방법을 제공하여야 하며, 1인당 1개를 초과하여 계정을 등록할 수 없다.

2. 사용자 계정의 삭제 또는 권한 변경 사유가 발생한 경우, 사용자는 정보시스템 담당자에게 통보하여야 한다.

3. 정보시스템 담당자는 검토, 승인 후 사용자 관리대장에 기록하고, 사용자 등록 후 결과를 신청한 사용자에게 통보한다.

4. 정보시스템 담당자는 월간 또는 분기별 단위로 사용자 등록 및 변경 현황을 유지한다.

5. 한 서버 시스템에 동일 사용자가 여러 계정을 등록할 수 없으며, 필요 시 정보시스템 당자에게 별도의 문서로 요청, 허가를 받아야 한다.

6. 정보시스템 담당자는 매 분기마다 사용자 계정에 대한 재확인을 실시하여 계정 삭제나 사용중지 등의 필요한 조치를 취하고, 그 결과를 소속부서 팀장에게 보고한다.

7. 사용자 계정의 재확인은 다음 각 목에 대하여 실시한다.

가. 퇴사 여부, 업무 필요성 여부

나. 마지막 사용일자가 60일을 초과하였을 경우

② 정보시스템 담당자는 허용된 계정의 취약성 예방을 위해 다음 각 호를 준수하여 계정을 보호하여야 한다.

1. 비밀번호가 없거나 비밀번호가 아이디와 동일한 계정을 허용해서는 안된다.

2. 시스템 담당자를 제외하고 관리자 계정이 존재해서는 안된다.

3. 반드시 필요한 계정을 제외하고는 유지보수사의 계정을 운영해서는 안 된다.

4. 모든 계정에 숨은 경로를 두지 않도록 한다.

5. 하나의 로그인 계정으로 동시에 여러 경로로 로그인 할 수 없다. 업무상 필요한 경우는 보안담당자의 동의하에 예외를 둘 수 있다.

6. 홈 디렉토리는 소유자 이외의 다른 사용자에게 쓰기 권한을 부여해서는 안된다.

7. 시스템 정보보호 및 사고 방지를 위해 주전산기에는 필수 사용자 이외에는 등록을 금한다.

③ 정보시스템 담당자는 서버 내 계정 정지 및 재사용시 다음의 각 호를 준수하여야 한다.

1. 어떠한 계정을 정지시킬 경우에는 그 사용자가 현재 로그온 중인지 확인해야 하고, 사용 중일 경우에는 반드시 로그아웃 하도록 하고 정지시켜야 한다.
2. 정지시켜야 할 계정에 대해 그 사용자가 현재 수행중인 프로세스가 있는지 먼저 점검하고, 수행 중일 경우에는 처리가 끝날 때까지 기다리거나, kill 등을 통해 중지시키고 계정을 정지해야 한다.
3. 재사용하는 사용자 계정은 새로운 비밀번호를 부여하고, 최초로 로그인을 할 때, 즉시 비밀번호를 변경하도록 해야 한다.

④ 정보시스템 담당자는 계정 폐쇄 시 다음 각 호의 사항을 이행하여야 한다.

1. 계정이 삭제(소멸)되는 사유 발생 시 즉시 삭제하도록 한다.
2. 계정 삭제는 다음 각 목의 사유에 따른다.

가. 사용자가 퇴직하는 경우

나. 소속 변경, 직무 변경으로 인한 사용 권한이 소멸되는 경우

다. 2개월 이상 미사용 계정(1개월 미사용시 계정을 정지시키고, 정지 후 1개월 내에 복원 요청이 없는 경우 삭제)

3. 삭제된 계정 사용자의 계층에 있는 모든 파일과 프로그램, 디렉토리 등을 제거한다.
4. 사용자가 파일 소유자로 되어 있는 모든 파일을 조사하여 불필요한 파일일 경우에는 삭제 한다.
5. 사용자가 만들어 놓은 예약 실행 설정 등을 점검하여 불필요한 파일을 제거한다.
6. 계정 내의 사용자 파일에 대한 접근 제어를 조사하여, 그 파일에 대해 접근 제어가 설정된 사용자들에게 통보하여 그 파일이 반드시 필요하지 않을 경우 삭제한다.
7. 별칭(aliases)으로 참조되는 사용자를 조사하여 적정성 여부를 판단하여 제거한다.
8. 사용자 계정이 관리 권한 밖인 다른 시스템 내에 존재하고 있을 경우, 그 정보시스템 담당자에게 그 계정에 대한 삭제를 의뢰하여야 한다.

⑤ 정보시스템 담당자는 계정 이동 시 다음 각 호의 사항을 고려하여야 한다.

1. 사용자의 UID와 GID가 있는지의 여부를 조사하고, 만일 존재할 경우에는 새로운 UID와 GID를 부여하여야 한다.
2. 계정에 대한 사용자 파일을 새로운 시스템으로 복사한다.
3. 이전의 계정은 폐쇄하거나 일시 정지시킨다.
4. 새로운 시스템으로 옮기려고 하는 계정이 관리 범위 밖의 계정이거나, 정보 보호가 취약한 곳으로 옮기려고 한다면, 사용자 파일에 대한 권한을 충분히 조사하여 적절하지 않을 경우 제거해야 한다.

⑥ 정보시스템 담당자는 서버 내 그룹 관리 시 다음 각 호의 사항을 준수하여야 한다.

1. 시스템에서 제공되는 그룹명은 기본적으로 사용한다.
2. 시스템 관리를 위해 구분된 그룹을 사용해야 할 경우에는 별도 구분하여 등록한다.
3. 업무별로 추가되는 사용자에 대해서는 업무별 그룹에 구분하여 등록한다.
4. 그룹명은 숫자로 시작하지 않아야 하며, 영문과 숫자를 조합하여 8자 이내로 구성한다.
5. 사용 목적이 유사하거나, 같은 프로젝트 내에 있는 사용자 계정은 동일한 그룹에 둔다.
6. 새로운 프로젝트가 생길 경우, 그 프로젝트에 관련된 사용자 단위로 그룹을 만든다.
7. 그룹 설정 및 비밀번호 설정 파일(예: /etc/group, /etc/passwd) 내에 있는 그룹과 사용자 계정은 서로 일치하여야 한다.
8. 특별히 보안을 요하는 사용자 계정에 대해서는 별도의 그룹을 지정한다.

9. 특정 업무를 위해 중복 그룹을 필요로 할 시에는 중복 그룹을 부여할 수 있다.
10. 구성원이 없는 그룹은 삭제한다. 만약 그 그룹 내에 파일이 남아있다면 새로운 그룹에 배정하거나 없애야 한다.

제19조(서버 소프트웨어 설치 관리) ① 정보시스템 담당자는 서버에 대한 소프트웨어 설치 및 변경 시 각 호의 사항을 고려하여야 한다.

1. 소프트웨어 설치 및 변경은 시스템 관리 담당자의 책임하 에 설치 및 변경한다.
2. 정보시스템 담당자는 소프트웨어 설치 및 변경 후에 반드시 정보보호 점검을 해야한다.
3. 설치 및 변경 시에 사용된 제조사 계정은 삭제한다.
4. 시스템 환경의 변화에 대하여 수시로 정보보호상의 허점이 없는지 점검해야 한다.
5. 소프트웨어 변경 후, 시스템 환경에 대한 백업이 정책에 따라서 이루어지는가 점검해야 한다.
6. 정보시스템 담당자는 시스템에 설치된 소프트웨어의 관리를 위해 목록표 등을 만들어 관리해야 한다.
7. 정보시스템 담당자는 보안성을 높이는 최신 패치를 설치한다.

② 정보시스템 담당자는 주기적으로 시스템 무결성을 점검하여야 하며, 다음 각 호에 대해 유의하여야 한다.

1. 비밀번호 파일(/etc/passwd 등)의 무결성 점검
2. 파일이나 디렉토리 허가 모드의 변경 사항 점검
3. 허가 받지 않은 Setuid, Setgid 파일의 존재 여부 점검
4. 자동실행 파일의 무결성 점검
5. 불법 소프트웨어
6. 바이러스, 백도어

③ 주요 시스템 파일 및 디렉토리는 일반 사용자가 쓰기 권한을 가져서는 안된다.

제20조(감사 및 로깅) ① 본 대학교 내 운영되는 모든 서버에 대해 사용자가 사용한 명령들에 대한 로깅은 중요 서버에 대해서만 수행하고, 기타 서버들은 요약 파일만 관리하도록 한다.

② 운영되는 정보시스템에 대해서 다음 각 호에 대해 기본적으로 로깅하여야 한다.

1. 가장 최근에 로그인한 사용자 정보
2. 사용자별 로그인 시간 정보
3. 사용자별 로그인/로그아웃 정보
4. 사용자별 접근 서비스 내용
5. 허가되지 않은 자산에 접근시 사용자 및 접근 내역
6. 허가되지 않은 사용자 침입시 침입자 정보/일시 등

③ 정보시스템 담당자는 로그 및 감사 관리를 위해 다음 각 호에 대해 유의하여야 한다.

1. 사용자나 이벤트 등의 감사 대상을 선택할 때 각 대상들의 적정성을 판단해야 한다.
2. 로깅 파일이 수용치를 넘을 때에는 테이프 등에 보관한다. 이 때 주요 시스템의 로 그 기록은 1년 이상 보관한다.
3. 최소한 주간 단위로 감사 로그 파일을 점검해야 한다.
4. 다음 각 목과 같은 비정상적인 행위에 대한 로그 파일은 주의깊게 점검하고 시스템 로

그 검토 결과서를 작성한다.

가. 최종 로그인 사용자

나. 로그인 실패

다. 시스템 파일에 대한 접근 실패

라. 정보보안과 관련되는 작업 수행에 대한 실패

마. 관리자 특권이 있는 파일 또는 서비스 사용 시도

바. 비인가된 파일, 자원 또는 서비스의 사용 시도

5. 시스템의 로그 기록이 불법 수정이 되지 않도록 보호하거나, 불법 수정을 확인할 수 있는 방법을 마련해야 한다.

6. 주기적으로 저장점검을 통해 감사 파일의 오버플로우를 예방해야 한다.

7. 로그 기록을 검토하여 침입 또는 침입 시도의 흔적 등 문제점이 있을 경우 본 시행 세칙의 침해사고 대응 절차에 따라 보안 관리자에게 보고하고, 기술된 절차에 따라 조치하여야 한다.

④ 정보시스템보안관리자는 정보시스템 담당자가 시스템에 대한 정보보안 업무를 수행하는지 분기 1회 이상 확인하여야 한다.

제21조(백업 및 종료) ① 정보시스템 담당자는 서버의 주요 정보시스템에 대한 백업 및 복구 정책을 적용 시 다음 각 호의 사항을 고려하여야 한다.

1. 중요 파일과 프로그램에 대해 주기적으로 테이프 백업을 받는다.

2. 백업의 주기 및 범위 등은 정보시스템 담당자와 프로그램 및 데이터의 소유자가 정한다.

3. 백업이 보관된 장소는 재난에 대비한 조치가 있어야 한다.

4. 필요시 복수의 백업을 만들어 소산해야 한다.

5. 다음 각 목의 내용은 시스템 변경시에 기본적으로 백업해야 할 파일들이다.

가. 환경 파일 및 저장 관리 데이터

나. 네트워크 서비스 구성 파일

다. 사용자 계정 관리 파일

라. 시스템 부트 파일

② 정보시스템 담당자는 시스템 종료(Shutdown) 시 다음 각 호의 사항에 유의하여야 한다.

1. 종료하기 전에 모든 사용자는 로그아웃 되어 있어야 한다.

2. 종료 명령어를 수행할 때 남아있는 사용자들이 로그아웃하고 프로세스가 끝날 수 있도록 적정한 주기를 설정해야 한다.

3. 마운트된 파일시스템을 물리적으로 쓰기 방지로 두지 않는다.

4. 디스크 드라이브 또는 다른 주변 장치에 대해 연결 해제 전 종료를 완료시켜야 한다.

제22조(주기적인 점검) 정보시스템 담당자는 서버 시스템에 대해 다음 각 호의 사항을 고려하여 주기적으로 점검하여야 한다.

1. 정보시스템 담당자는 주기적으로 보안 점검 체크리스트를 이용하여 보안 점검을 수행하고, 점검 결과서를 매월 소속부서 팀장에게 제출한다.

2. 서버에서 운영 중인 서비스를 조사하여 인가받지 않고 추가나 변경이 이루어진 서비스

가 존재하는 지 조사한다.
3. 쉘을 수행하는 프로그램 목록을 조사한다.
4. 추가된 계정, 비밀번호의 생략, UID 변경여부를 확인한다.
5. 해킹된 시스템이 존재하는 경우 네트워크에 연결되어 있는 다른 시스템에도 피해가 있는지 확인한다.

제23조(서버 침해사고 대응 절차) 불법적인 침입자나 침입 징후의 발견 시 대응절차는 제3장 침해사고 대응에 의거한다.

제8장 웹 보안

제24조(홈페이지 개발) 본 대학교에서 개발 및 운영되는 모든 홈페이지는 다음 각 호의 사항을 준수하여야 한다.
1. 모든 홈페이지는 기본적인 취약점이 제거되어야 하며, 이를 위해 교육사이버안전센터의 “웹 서버 및 홈페이지 취약점 점검 가이드”를 준수한다.
2. 중앙대학교 통합인증(SSO/SLO) 적용 시 개발팀의 “SSO/SLO 인증 가이드”를 따르며, 연동에 따르는 보안 취약점을 제거하여야 한다.
3. 홈페이지 자체인증을 위해 회원가입을 받아 처리하는 경우 “개인정보보호법” 및 “개인정보보호규정”에서 말하는 개인정보처리시스템으로 분류하여, 개인정보영향평가 및 안전성확보조치에 관한 의무 사항을 이행하여야한다.
4. 사용자 및 관리자 로그인을 위한 인증 기능 구현 시 송수신되는 비밀번호는 네트워크 구간에 암호화(SSL 또는 암호처리 기능 구현)되어 전송되어야 한다.

제25조(홈페이지 및 정보시스템 개발 기술검수) ① 본 대학교와 관련된 자원(명칭, 예산, 인력, IT자원) 중 한 가지 이상을 활용한 홈페이지 등 정보시스템을 구축(개설/개편) 및 운영하려는 경우, 다음 각 호를 준수하여 사전 심의 및 허가를 득하여야 한다.
1. 개발 계획 수립 및 협의 : 운영부서담당자, 개발사, 지원부서담당자
2. 임시 개발 서버(호스팅 포함) 구축 및 도메인 가배정 : 운영부서담당자, 개발사, 정보시스템 및 네트워크담당자
3. 개발 : 운영부서담당자, 개발사
4. IT기술검수 (취약성 및 개발 프로세스 점검) : 운영부서담당자, 개발사, 정보시스템담당자, 개발부서담당자
5. 홈페이지 및 정보시스템 운영(실서버 이전 및 도메인 활성) : 운영부서, 정보시스템담당자, 네트워크담당자

② 네트워크담당자는 홈페이지 용도(A) 외 도메인 명을 배정하지 않는다. 단, 본 대학교 대다수 구성원과 관련된 서비스 및 정보통신센터의 정보시스템에 대해서는 예외로 한다.

③ 정보시스템담당자는 홈페이지 개발을 위한 임시 개발서버 및 호스팅 서비스(웹, 빌더, 서버)를 제공하며, 웹취약성 점검 및 개인정보보호 관련 체크리스트를 점검한다.

④ 개발부서 담당자는 개발 상 고려해야 할 취약성 및 표준 개발절차가 적용되었는지 점검한다.

⑤ 정보시스템보안담당자 및 개인정보보호담당자는 각 심의 절차가 적절히 수행되었음을

점검하며, 미비한 사항 발견 시 각 담당자를 통해 재점검을 의뢰할 수 있다.

⑥ 정보통신센터장은 모든 심의 절차가 완료되었을 때에 신청된 홈페이지 운영에 대해 최종 허가한다.

제26조(취약성 점검) 본 대학교의 모든 홈페이지에 대해 정기 또는 수시로 취약성 점검을 시행하여 홈페이지 취약점 및 개인정보노출 발견 시 다음 각 호에 따라 조치한다.

1. 1차 발견 : 유선 또는 서면(공문, 전자우편) 등 서면 조치 요청 및 경고
2. 2차 발견 : 1차 경고 후 3일 이내 미 조치 시 계정, IP 및 도메인 서비스 차단

제27조(침해사고 대응) 본 대학교에서 운영 중인 홈페이지 및 웹시스템에 대한 침해사고 발생 시 다음 각 호에 따라 대응하여야 한다.

1. 웹 보안사고 발생 시 중요도 및 시급성에 따라 호스팅 담당자는 사용자의 동의없이 계정 서비스를 임시 중지할 수 있다.
2. 보안사고가 발생한 홈페이지의 담당자는 최선을 다해 피해 최소화 및 복구작업을 수행하여야 하며, 호스팅 담당자는 이를 지원한다.
3. 홈페이지 담당자는 복구된 홈페이지에 대해 보안 취약성이 개선되었음을 호스팅 담당자에게 입증하여야 한다.
4. 호스팅 담당자는 복구된 홈페이지 및 서버에 대해 취약성이 개선되고, 보안 준수사항이 이행되었다고 판단할 경우 웹서비스를 재가동 할 수 있다.
5. 정보시스템보안담당자 및 호스팅 담당자는 필요 시 중요 홈페이지에 대해 교육부 교육사이버안전시스템을 통한 보안취약성 점검을 추가로 실시할 수 있다.
6. 기타 대응절차는 제3장 침해사고 대응을 따른다.

제9장 전자우편 보안

제28조(전자우편 사용) ① 본 대학교에서 제공하는 전자우편 계정은 인트라넷(중앙대포탈 및 그룹웨어)에서 전자우편 계정을 온라인으로 신청한다.

② 전자우편 사용을 위해 다음 각 호의 사항이 준수되어야 한다.

1. 전자우편을 상업적인 용도로 사용해서는 안된다.
2. 본 대학교의 학생, 교원, 직원은 전자우편을 사용할 수 있으며, 예외의 경우 정보통신센터장의 승인을 득한다.
3. 비밀 또는 학교가 소유한 정보는 전자우편으로 보내지면 안된다.
4. 외부 사용자가 계정을 탈취하여 전자우편을 발송하는 경우 전자우편 시스템 담당자가 임의로 비밀번호변경이나 메일 발송중지 조치를 할 수 있다.
5. 고의로 전자우편을 오용하는 경우 상응하는 징계조치를 취한다.

제29조(전자우편 관리) 본 대학교의 전자우편 시스템 담당자는 전자우편 시스템 구축 시 다음 각 호를 유의하여야 한다.

1. 전자우편 서버의 비밀번호는 “제11장 계정 및 비밀번호 보안”의 비밀번호 보안규칙을 따른다.
2. 익명 remailer 소프트웨어는 설치할 수 없다.
3. 전자우편 서버는 검증된 발신 주소가 아닌 전자우편을 거절하도록 한다.
4. 전자우편 메시지의 내용은 범죄 조사, 보안취약성 조사, 감사를 위한 경우를 제외하고 비밀로 간주한다.
5. 받는 메시지의 경우 전자우편서버에서 첨부 파일에 대한 바이러스 검사를 실시한다.
6. 전자우편 시스템 관리자는 전자우편관련 보안문제나 외부 해킹공격 등의 발견 시 정보시스템보안담당자에게 즉시 알려야한다.

제10장 데이터베이스 보안

제30조(DB 인증) ① 본 대학교 내의 DB 시스템은 다음 각 호의 인증정책을 적용하여야 한다.

1. DB 담당자는 계정 및 비밀번호 관리에 대한 책임과 권한을 갖는다.
2. DB에의 접근은 항상 인증을 통해서만 가능하도록 한다. 이를 위해 인증 모듈은 DB를 구동시키는 즉시 제공되어야 하며 항상 활성화되어 있어야 한다.
3. DB의 접근제한을 위해서는 역할을 통해 사용자 및 사용자 그룹을 등록하여야 한다.
4. 각 사용자는 비권한자의 사용을 방지하기 위해 비밀번호가 설정되어야 한다.
5. 각 사용자 DB에 연계된 사용자는 ID와 동일한 이름의 스키마를 가져야 한다.

② DB 시스템의 계정 관리 시 DB 담당자는 다음 각 호를 준수하여야 한다.

1. DB를 사용하고자 하는 자는 DB 담당자에게 문서화된 사용신청을 하고 DB 담당자는 타당성 검토를 한 후 계정을 부여한다.
2. 장기 파견자, 휴직자는 업무에서 신속히 제거한다.
3. DB 담당자는 퇴직자 발생 시 즉시 계정을 삭제하여야 한다.
4. 기본 생성된 계정은 설치 후 업무에 사용되지 않는다면 삭제하도록 한다.
5. 본 대학교의 주전산기의 DB는 필요한 최소한의 범위 내에서 계정을 생성한다.
6. DB 담당자는 사용자 관리대장을 작성 및 유지하여야 한다.
7. 비밀번호가 없는 계정은 사용을 금한다.
8. DB 담당자 권한을 가지고 있던 사용자가 인사발령, 퇴직 등의 사유로 다른 곳을 옮길 때에는 인수자는 즉시 관리자 계정 및 비밀번호를 변경하도록 한다.
9. 잘못된 로그인 회수에 제한을 두어 제한된 수를 넘을 경우 자동적으로 연결을 해제한다.
10. 일정 시간동안 작업이 없으면 자동으로 로그아웃 되도록 한다. 단, 업무상의 필요성이 있는 경우 예외를 둔다.

제31조(DB 접근제어) ① DB 관리자는 다음 각 호에 따라 접근수준 및 권한부여를 한다.

1. 사용자가 DB 파일에 접근할 수 있는 수준은 보안관리 규정에 따른 정보보호 등급과 사용자의 접근 권한에 따라 DB 담당자가 결정해야 한다.
2. DB 담당자는 사용자의 시스템 자원 사용 수준을 결정해야 한다.
3. DB 담당자는 테이블에 행위별 권한, 필드 접근 권한 등의 객체 권한을 조정해야 한다.
4. 시스템 권한은 DB 담당자만이 가진다.
5. 저장 프로시저 및 툴을 사용하여 설정된 접근권한을 체크하고 수정한다.
6 접근제어에 대한 설정은 DB 담당자의 허가를 득하고서만 변경될 수 있도록 한다.
7. 접근제어에 대한 설정은 환경의 변화 등을 반영하여 주기적으로 갱신한다.

② DB 관리자는 다음 각 호에 해당하는 접근제어 메커니즘을 DB에 적용한다.

1. DB의 중요성과 특성에 맞는 접근제어 메커니즘을 택하여 적용한다.
2. 메커니즘에 맞는 구체적인 접근제어 절차를 마련한다.
3. 주체와 객체의 권한, 접근 시도 장소 및 시간 등에 따른 접근제어를 실시한다.
4. 필요한 경우 관리 툴을 이용하여 접근권한을 설정/통제한다.
5. 사용하지 않는 계정에 대해서는 주기적으로 검사하고 권한을 적절히 제한하도록 한다.
6. 사용자와 업무에 관한 권한 정보는 문서화되어 관리되며 항상 최신의 상황을 반영하도록 갱신되도록 한다.

③ 운영되는 DB 시스템 내의 데이터는 다음 각 호를 고려하여 암호화하여야 한다.

1. 기밀성이 요구되는 DB 시스템 내의 중요 필드에 대해 암호화하여야 한다.

2. 암호화를 지원할 수 있는 암호화 기술이 DB 시스템에 도입되어야 한다.
3. DB로 기밀성이 요구되는 데이터를 전송할 때에는 암호화되어야 한다.
4. DB로의 암호화 전송을 지원할 수 있는 전송 시스템이 도입되어야 한다.

제32조(로깅 및 감사) ① 본 대학교 내 운영되는 DB 시스템은 다음 각 호를 고려하여 로깅되어야 한다.
1. 사용자의 로그인 시간 및 로그인 지속 시간이 적절한 범위 내에서 로깅 되어야 한다.
2. DB에 연결된 사용자의 수가 적절한 범위 내에서 로깅되어야 한다.
3. 접속에 실패한 접근 시도가 로깅되어야 한다.
4. 기타 모든 이벤트에 대해 로깅되어야 한다.

② DB 시스템에 대한 감사를 위해 다음 각 호의 사항은 준수되어야 한다.
1. 기록된 로그파일은 DB 관리자에 의해서 정기적으로 점검되어야 한다.
2. 점검이 이루어진 로그파일은 정기적으로 삭제되어야 한다.
3. 로그파일의 분석을 위하여 관리자가 부가적인 도구를 설치 사용할 수 있다.
4. 로그/감사에 대한 엄격한 접근제어를 실시한다.
5. 중요 DB의 경우 DB 담당자와 DB 관리자의 권한을 분리한다.
6. 로그파일의 조작 및 읽기 권한은 DB 관리자에게만 있어야 한다.
7. 로그파일의 무결성을 보장하기 위하여 로그파일 자체에 대한 모니터링을 주기적으로 실시한다.

제33조(사고 대응 절차) 불법적인 침입자나 침입 징후의 발견 시 대응절차는 제3장 침해사고 대응에 의거한다.

제11장 계정 및 비밀번호 보안

제34조(계정 및 비밀번호 생성) ① PC 및 정보시스템에 대한 사용자 계정 및 비밀번호 생성 시 다음 각 호에 대해 유의해야 한다.
1. 모든 시스템의 계정은 각 시스템의 용도에 맞도록 그 사용권한을 적절히 지정하여야 한다.
2. 계정 사용자의 비밀번호는 비밀로 유지하고 타인에게 노출하지 않도록 한다
3. 생성 및 변경되는 모든 비밀번호는 복호화가 불가능하도록 일방향 암호화되어 저장되어야 한다.
4. 사용자가 관리자에게서 임시 비밀번호를 부여 받은 경우 비밀번호를 변경해야 한다.
5. 비밀번호를 별도의 문서에 적어 놓거나 암호화되지 않은 형태로 PC에 저장해서는 아니 된다.
6. 비밀번호는 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하여야 하며, 다음 각 목의 기준을 따른다.

가. 10자리 이상 : 영대문자, 영소문자, 숫자 및 특수문자 중 2종류 이상 구성한 경우
나. 8자리 이상 : 영대문자, 영소문자, 숫자 및 특수문자 중 3종류 이상 구성한 경우
영문과 숫자 특수문자를 혼용해 8자 이상의 비밀번호를 사용한다.

7. 주민번호, 전화번호, 생일, 사전에 나오는 단어 등 임의 추측이 가능한 비밀번호를 피하

고 문장의 첫 글자 조합을 이용하는 등의 방법으로 비밀번호를 만든다.

8. 시스템 개발 이관 및 소프트웨어 설치 후 공급자가 설정한 기본 비밀번호는 반드시 변경한다.
9. 비밀번호가 타인에게 노출되었거나 노출이 우려될 경우 반드시 비밀번호를 변경해야 한다.
10. 사용자는 개인PC 및 정보시스템을 사용하거나 본인 계정으로 정보통신망에 접속하는 것과 관련한 보안책임을 가진다.

제35조(비밀번호 관리) ① 사용자가 시스템 사용에 대한 권한을 부여받을 때에는 반드시 비밀번호를 받도록 해야하며, 다음 각 호의 사항이 준수되어야 한다.

1. 사용자의 비밀번호는 주기적으로 변경해야 한다.
2. 사용자는 자신의 비밀번호를 기억하고 있어야 하고, 비밀번호에 대한 보안을 철저히 해야 한다.
3. 모든 사용자는 비밀번호 인증을 통해서만 시스템을 사용할 수 있도록 한다.
4. 비밀번호는 최초 생성/변경 후 최소 6개월 내 변경하여야 하며, 직전의 비밀번호로는 변경이 허용되지 않아야 한다.
5. 모든 사용자의 비밀번호 입력 제한은 5회 이하로 하고, 실패시 자동적으로 연결을 해제시키고, 사용자 계정은 사용 중지시키며 비밀번호 찾기 이후 다시 사용할 수 있도록 한다.
6. 시스템 관리자 권한을 갖고 있던 사용자가 퇴직 등의 사유로 다른 곳으로 옮길 때에는 인수자는 즉시 기존에 사용했던 비밀번호를 변경해야 한다.
7. 시스템 관리 담당자는 수시로 비밀번호 파일에 대한 접근 권한을 점검한다.

② 시스템 관리자는 다음 각 호의 사항을 수행하여야 한다.

1. 신규 사용자가 통합아이디 발급이 원활하도록 지원한다.
2. 비밀번호의 변경주기 시마다 교체할 수 있도록 지원한다.
3. 퇴직자들에게는 최소한의 서비스만 제공(메일 등)하며, 그 범위는 총장이 따로 정의한다.

③ 모든 사용자는 다음 각 호의 사항을 준수해야 한다.

1. 자신의 비밀번호는 항상 보안을 유지하여야 한다.
2. 비밀번호를 다른 곳에 기입해 두지 말아야 하며 항시 기억하고 있어야 한다.
3. 의심스러운 비밀번호 위반이나 변화가 발생할 때에는 즉시 보안관리자나 시스템 관리 담당자에게 보고해야 한다.
4. 다른 사람이 지켜보고 있는 상태에서 비밀번호를 입력하지 말아야 한다.
5. 계정이 여러 서버에 있을 경우에는 각각 다른 비밀번호를 선택해야 한다.
6. 비밀번호는 최소 6개월에 한번 바꾸어야 한다.

제37조(정보시스템 관리자 계정 및 비밀번호 관리) ① 정보시스템에 대한 관리자 계정은 관리자 외에 사용을 할 수 없으며, 타인에게 빌려주지 못한다. 특별한 사유로 타인이 사용하는 경우 사용 후 반드시 비밀번호를 변경하여야 한다.

② 정보시스템 관리자의 비밀번호는 다음 각 호를 준수하여 관리되어야 한다.

1. 관리자 계정의 비밀번호는 최소한 3 개월에 한번 바꾸어야 한다.

2. 시스템의 관리자 비밀번호에 대해서는 시스템 관리자 계정 및 비밀번호 현황 대장에 기록하고 비밀문서로 취급하여 안전한 금고에 보관하며, 인가된 자 외에는 열람을 차단하여야 한다.
3. 분기별로 시스템 관리 담당자는 변경된 관리자 비밀번호를 밀봉하여 정보시스템보안관리자에게 제출하고, 정보시스템보안관리자는 내역을 기록한 후 금고에 보관한다. 긴급 필요시 인프라팀장의 지명을 받은 업무담당자는 정보시스템보안관리자에게 밀봉된 관리자 암호를 요청하고. 승인을 득한 후 개봉하여 사용한다.

제12장 바이러스 및 악성코드 보안

제38조(바이러스 관리) 바이러스로 인한 피해를 최소화하기 위해 사용자와 업무담당자는 다음의 각 호의 사항을 준수해야 한다.
1. 비 인가된 소프트웨어 및 불법 소프트웨어 사용을 금지한다.
2. 외부 네트워크나 매체로부터 파일이나 소프트웨어를 다운로드 받을 경우 백신 프로그램을 적용한 후 사용한다.
3. 백신 프로그램을 설치하고 정기적으로 업데이트를 수행한다.
4. 중요 시스템의 소프트웨어 및 데이터는 주기적으로 점검하여 허가되지 않은 파일이나 수정사항 등이 있는지 조사한다.
5. 전자우편 첨부 파일에 대한 바이러스 감염여부를 점검한다.
6. 소프트웨어가 바이러스에 감염되는 것을 방지하기 위해 원본 소프트웨어는 쓰기 방지가 되어 있어야 한다.
7. 시스템의 바이러스 감염 시 즉각 담당자에게 통지한다.
8. 백업담당자는 바이러스 공격에 의한 피해를 복구하기 위한 적절한 백업, 복구계획을 수립한다.
9. 악성 소프트웨어에 대한 새로운 정보 및 보호 대책에 대해 사용자에게 주기적 혹은 수시로 공지한다.

제39조(바이러스 관리 절차) ① 본 대학교 내의 바이러스 유포 및 예방을 위해 소프트웨어 담당자와 사용자는 다음 각 호의 사항을 준수하여야 한다.
1. 소프트웨어 담당자는 바이러스를 예방 및 제거할 수 있는 최신 버전의 백신 프로그램을 배포한다.
2. 사용자는 현재 사용 중인 컴퓨터가 바이러스에 감염되었는지 확인할 수 있도록 백신 프로그램을 설치하고 주기적으로 업그레이드 한다.

② PC 및 정보시스템에 설치된 백신 프로그램은 다음 각 호를 고려하여 실행되어야 한다.
1. 사용자는 외부저장장치 및 다운로드를 통해 외부에서 반입되는 파일은 사용 전 반드시 바이러스의 감염 여부를 검사하고 바이러스 발견 시 이를 완전히 제거 후 사용한다.
2. 사용자는 전자우편 첨부 파일에 대한 바이러스 감염 여부를 검사하고 바이러스 발견 시 이를 완전히 제거 후 사용한다.
3. 사용자는 제3자에게 소프트웨어를 제공하기 전에 바이러스나 프로그램 오류 등이 있는지 검사하여야 한다.
4. 사용자는 주기적으로 백신 프로그램을 실행하여 점검한다.

제13장 휴대용 저장매체 및 데이터 관리 보안

제40조(휴대용 저장매체) ① 휴대용 저장매체는 이동식 저장장치를 포함하며, 이를 이용한 중요 자료를 보관할 필요가 있을 때에는 소속부서 관리책임자의 승인을 받아야 한다.
② 각 부서의 관리책임자는 이동식 저장매체는 중요 자료 및 개인정보 자료를 관리하기 위한 비밀용과 일반 용도의 사용을 위한 일반용으로 구분하고, 주기적으로 수량 및 보관 상태를 점검하여야 한다.
③ 교내에서 휴대용 저장매체를 PC 등에 연결하여 사용 시 반드시 백신 프로그램이 자동 구동되어 바이러스 및 악성코드 감염 여부를 먼저 확인하여야 한다.
④ 휴대용 저장매체를 파기 등 불용처리 할 경우, 저장되어 있는 정보의 복구가 불가능하도록 완전삭제 프로그램을 사용하여 초기화를 하거나, 물리적으로 파손시켜야 한다.
⑤ 정보보호시설에서 휴대용 저장매체를 사용할 경우, 정보시스템보안담당자 및 업무담당자의 승인을 받아야 하며, 휴대용 저장매체 반출입대장에 기록하여야 한다.

제41조(데이터 관리) ① 교내의 업무, 개인정보, 비밀 자료를 교외 기관, 회사에서 운영하는 전산시스템(전자우편 시스템, 홈페이지, 소셜네트워크서비스(SNS) 및 클라우드 시스템 등)에 보관해서는 아니 된다.
② 불가피하게 외부의 정보시스템에 자료를 보관해야 할 경우, 정보시스템보안담당관의 허가를 받아야 한다.
③ 본 대학교의 행정업무에 사용되는 모든 정보는 학교 자산으로 등록된 정보화기기에만 사용이 가능하며, 개인 소유의 정보화기기에 저장할 수 없다.

제14장 보칙

제42조(준용) 이 시행세칙에 명시되지 않은 사항은 교육부 정보보안기본지침과 본 대학교의 “개인정보보호 규정”, “보안규정”을 준용한다.

부칙

(시행일) 이 시행세칙은 2016년 3월 2일부터 시행한다.

부칙

(시행일) 이 개정 시행세칙은 2017년 6월 1일부터 시행한다.

붙임 #1 사이버 침해 사고 신고 서식

사 고 신 고

<table>
<tr><td colspan="4">기 본 정 보</td></tr>
<tr><td>기 관 명</td><td>대신대학교</td><td>부 서</td><td></td></tr>
<tr><td>성 명</td><td></td><td>직 위</td><td></td></tr>
<tr><td>전자우편</td><td colspan="3"></td></tr>
<tr><td>연 락 처</td><td colspan="3">전화 : Fax :</td></tr>
<tr><td colspan="4">사 고 내 용</td></tr>
<tr><td rowspan="2">사고일시</td><td>년 월 일</td><td rowspan="2">피해IP주소</td><td rowspan="2"></td></tr>
<tr><td>시 분</td></tr>
<tr><td rowspan="2">피해시스템 용도</td><td rowspan="2">< >
* 뒷장의 ‘가. 시스템분류’ 기호입력</td><td rowspan="2">운영체제</td><td>□윈도우 □유닉스 □네트워크장비</td></tr>
<tr><td>상세버젼정보 :</td></tr>
<tr><td>사고 유형</td><td>< >
* 뒷장의 ‘나. 사고유형’ 기호입력</td><td>피해범위</td><td>< > 대
* 피해시스템이 여러대인 경우 피해숫자 기입</td></tr>
<tr><td>사고 내용</td><td colspan="3"></td></tr>
<tr><td colspan="4">조 치 내 용</td></tr>
<tr><td>공격자 정보</td><td colspan="3"></td></tr>
<tr><td>피해 현황</td><td colspan="3"></td></tr>
<tr><td>긴급조치
실시사항</td><td colspan="3"></td></tr>
<tr><td>관련보안제품
운영현황</td><td colspan="3"></td></tr>
<tr><td colspan="4">그 밖에 사고 관련 내용을 구체적으로 서술</td></tr>
<tr><td colspan="4"></td></tr>
</table>

가. 시스템 분류 목록

기호	시스템 분류	설 명
가	웹서버	기관의 홈페이지 운영 및 웹서비스를 제공하는 서버
나	전자우편 서버	전자우편 송수신을 위해 운영하는 서버
다	DB/업무서버	홈페이지 및 업무지원을 위한 데이터베이스 서버
라	개발/임시서버	개발 및 운영 테스트를 위하여 사용하는 임시 서버
마	통신전송장비	라우터, 스위치 등 통신전송장비 일체
바	보안장비	방화벽, IDS, VPN 및 백신서버 등 정보보안제품 일체
사	개인/업무PC	기관내 사용자의 PC
아	교육/임시PC	교육장 또는 공용 작업을 위해 여러 명이 사용하는 PC
자	기타	위의 시스템 용도에 없는 경우 서술식으로 기술

나. 사고 유형 목록

기호	사고 유형	설 명
A	경유지 악용	타기관으로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹흔적 또는 해킹툴이 설치되어 타 시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 스스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단 송신된 흔적이 발견되었을 경우
C	단순침입 시도	지속적인 스캐닝 공격이 발생할 경우
D	웜바이러스 피해	기관내의 PC에서 웜바이러스가 발견되었을 경우
E	홈페이지 변조	기관의 홈페이지가 변조되었을 경우
F	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네트워크 이상으로 인해 홈페이지 접속이 불가능 할 경우
G	서비스 거부 공격 피해	불특정 다수의 IP로부터 접속시도 또는 대량 트래픽이 일시에 유입될 경우
H	기타	위의 사고유형에 포함되지 않을 경우 서술식으로 기술

붙임 #2 보안서약서 서식

개인정보 처리 업무 위탁 보안 서약서

_____(이하 “을”이라 한다)는 대신대학교(기관)(이하 “갑”이라 한다)의 개인정보 처리 업무 위탁 업무 수행에 따른 개인정보 및 개인정보처리시스템의 안전한 보호를 위해 아래 각 호의 사항을 준수한다.

1. 을은 갑이 위탁한 개인정보 처리 업무 수행 시 개인정보(정보 및 정보시스템)를 안전하게 사용·관리하며, 개인정보의 보호를 위해 다음의 사항을 준수한다.
  1) 갑의 정보보안 기본지침 및 개인정보보호 관련 법령 준수
  2) 개인정보 위탁 업무 처리 시 기술적·관리적 보호 조치
  3) 위탁 업무 수행 목적 외 개인정보의 처리 금지
  - 위탁 업무의 목적 :
  - 위탁 업무의 범위 :
  - 위탁 업무의 범위 :
 4) 갑이 위탁한 개인정보 처리 업무의 재 위탁 제한(제 3자 공유 금지)
 5) 개인정보에 대한 접근 제한 등 안전성 확보 조치 준수(개인정보보호법 제29조 및 동법 시행령 제30조)
 6) 위탁 업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 및 감독 철저
 7) 위탁 업무의 종료 시 개인정보 파기 등 의무사항 이행
 8) 을은 갑의 규정 및 관련 법령의 미 준수 또는 관리 소홀로 인해 발생하는 제반 사고에 대한 책임을 부담한다.

2. 을은 갑의 업무 수행을 위해 담당하는 직원에 대하여 책임을 진다
3. 을은 갑의 사전 승인을 받지 못한 프로그램 및 정보기기는 갑의 업무와 관련하여 사용하지 않는다.
4. 을은 갑의 정보보호 정책과 반하는 행위로 야기되는 문제에 대해 민·형사상의 책임을 진다.

상기 사항을 숙지하고 이를 성실히 준수할 것을 서약 함.

년 월 일

위탁 업체 대표 : (인)